SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

# Standards Navigator

## Standards Navigator Monthly Report

## 4-March-2015

SoftwareCPR Standards Navigator provides information and tools related to standards that play a significant role in health software and software intensive medical devices. In addition to information on existing standards, SoftwareCPR Standards Navigator keeps you up to date on new standards activity and gives you expert insight into future changes to existing standards.

http://www.softwarecpr.com/topicsframepage.htm

# February 2015 Standards Navigator Overview

**Medical device software**

- No new documents this month. The FDIS for IEC 62304 Amendment 1 is being edited by IEC and should be circulated soon for a 2 month final vote. Work on the second edition of IEC 62304 has begun and a committee draft is expected by the end of this year.

**Medical Devices**

- IEC 62366-1: Medical devices – Part 1: Application of usability engineering to medical devices was approved. This new standard will replace IEC 62366:2014. It will be published this spring.
- A second draft for vote (DIS) of the third edition of ISO 13485 has been circulated. This third edition will replace ISO 13485:2003. It is based on, and follows the format of, ISO 9001:2008.

  *The draft standard is available on the SoftwareCPR Standards Navigator web page.*
- IEC has initiated a review of IEC 60601-1 and its associated collateral standards (IEC 60601-1-2 through IEC 60601-1-12) in preparation for beginning an update to this series of standards. The stability date for IEC 60601-1 will remain 2019, but the revision process is expected to begin in late 2015 or 2016. National committees have been asked to review every document in light of its place in, and its interactions with the other documents that make up the whole of the "general standard". In their review, National Committees are requested to identify issues considering the need to:

  A. Address the changes needed to stay current with the generally acknowledged state of the art. For example, IEC 60950-1, on which many requirements in the "general standard" are based, is being supplanted by IEC 62368-1, *Audio/video, information and communication technology equipment - Part 1: Safety requirements*. Should the relevant requirements in IEC 60601-1 remain aligned with the latest edition of IEC 60950-1, comply with both IEC 60950-1 and IEC 62368-1, or fully adapt to the new terminology and structure of IEC 62368-1?

  B. Tackle unaddressed safety aspects in the third edition of IEC 60601-1 or any of the collateral standards. For example, any of the issues submitted to IEC/SC 62A/WG 14 along with the recommendations/interpretations developed by WG 14 to be published in the forthcoming Technical Report, IEC TR 60601-4-3, *Medical electrical equipment – Part 4-3: Guidance and interpretation – Considerations of unaddressed safety aspects in the third edition of IEC 60601-1 and proposals for new requirements.*

  C. Address inconsistencies or ambiguities between sections of Part 1, between Part 1 and any of the collateral standards, or between individual collateral standards. For example, consider the ambiguity regarding the colour of indicator lights and their meanings as described in Table 2 IEC 60601-1:2005 and the requirements for visual alarm signals on 6.3.2 of IEC 60601-1-8:2006+A1:2012.

**Health IT and mobile health applications**

- No new documents.

**Quality**

- A second draft for vote (DIS) of the third edition of ISO 13485 has been circulated. This third edition will replace ISO 13485:2003. It is based on, and follows the format of, ISO 9001:2008.
  *The draft standard is available on the SoftwareCPR Standards Navigator web page.*

**Security**

- The new work item proposed for a technical report on using assurance cases to demonstrate security capability was approved. Work on *IEC/TR 80001-2-9 Ed. 1.0 Application of risk management for IT networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities* will begin in April. Publication is expected by the end of 2016.

**Software Engineering and Information Technology**

- A third committee draft for comment (CD) of ***ISO/IEC 12207 - Systems and software engineering — Software life cycle processes*** has been circulated. This new revision of ISO/IEC/IEEE 12207 is the product of a coordinated effort by IEEE and ISO/IEC JTC 1/SC 7 to completely harmonize life cycle process standards for systems and for software. The new editions of ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 will provide a single, shared baseline of systems and software life cycle processes applicable to both the ISO/IEC and the IEEE standards collections. This standard will be reviewed by the IEC 62304 second edition project and the 80001-1 revision project to understand how those standards could be better aligned with the processes in ISO/IEC 12207.

  *The draft standard is available on the SoftwareCPR Standards Navigator web page.*

- A final draft for vote (FDIS) of ***ISO/IEC 33063 - Information Technology — Process Assessment — Process assessment model for software testing*** has been circulated. This standard provides an example of a process assessment model for software testing for use in performing a conformant assessment in accordance with the requirements of 'ISO/IEC 33002 – Process Assessment – Requirements for performing process assessments'. The process reference model defined in 'ISO/IEC/IEEE 29119-2 - Software and Systems Engineering — Software Testing — Part 2: Test Processes' has been used as the basis for the ISO/IEC 33063 exemplar process assessment model for software testing. ISO/IEC 33063 contains a set of indicators to be considered when interpreting the intent of the Process reference model. These indicators may also be used when implementing a process improvement program or to help evaluate and select an assessment model, methodology and/or tools.

  *The draft standard is available on the SoftwareCPR Standards Navigator web page.*

- A third committee draft of ***ISO/IEC 25011 Information technology — Service Quality Requirements and Evaluation (SQuaRE) — Service Quality Model*** has been circulated. This International Standard defines a quality model for services that use IT made up from a combination of resources including people, processes, technology, facilities and information. The model is composed of characteristics (which are further subdivided into subcharacteristics) that can be used to support the requirements definition, design, deployment, delivery and improvement of services that use IT. It also provides guidelines for applying the quality in use model included in ISO/IEC 25010 to services. The quality characteristics and subcharacteristics, which are defined in the quality model, provide a consistent terminology for specifying, measuring and evaluating IT service quality.

  *The draft standard is available on the SoftwareCPR Standards Navigator web page.*

- A proposal has been circulated for a new work item to revise *ISO/IEC 19770-1 Information technology – IT asset management – IT asset management systems – Requirements* to cover the same process areas that were covered in ISO/IEC 19770-1:2006 and ISO/IEC 19770-1:2012, but with them rearranged and redefined to meet the requirements for Management System Standards (MSS) and to better integrate with the ISO 55000 family of Asset Management standards. A draft CD is included with the proposal. ISO/IEC 19770-1 specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for IT asset management, referred to as an "IT asset management system".

  *The NP form and the draft CD are available on the SoftwareCPR Standards Navigator web page.*

## STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

| | Topic | Use / Users | Description |
|---|---|---|---|
| ISO/IEC/IEEE 15289 FDIS | Software Engineering | Manufacturers | ISO/IEC/IEEE FDIS 15289 Software and Systems Engineering — Content of life cycle information items (documentation)<br><br>The purpose of ISO/IEC/IEEE15289 is to provide requirements for identifying and planning the specific information items (documentation) to be developed and revised during systems and software life cycles and service processes. (2015-3-21) |
| ISO/IEC 19770-5 FDIS | Software Engineering | Manufacturers | ISO/IEC FDIS 19770-5 Information technology – IT asset management – Overview and vocabulary<br><br>This International Standard provides an overview of software asset management, which is the subject of the ISO/IEC 19770 family of standards, and defines related terms. (2015-05-03) |
| ISO/IEC 25023 DIS | Software Engineering | Manufacturers | ISO/IEC DIS 25023 Systems and software Engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality<br><br>This International Standard is a part of the SQuaRE series of international standards. It provides a set of measures for the characteristics of system/software products that can be used for specifying requirements and measuring and evaluating the system/software product quality. (2015-05-09) |
| ISO/IEC 19770-4 NWIP | Software Engineering | Manufacturers | ISO/IEC NWIP 19770-4 Information technology — IT asset management — Resource utilization measurement<br><br>This part of ISO/IEC 19770 provides an International Standard for resource utilization measurement (RUM). A RUM is a standardized structure containing authoritative usage information about the consumption of resources that are related to the use of a software asset. (2015-3-20) |

# STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

| | Topic | Use / Users | Description |
|---|---|---|---|
| ISO/IEC NWIP | Software Engineering | Manufacturers | NWIP Systems and Software Engineering- Guideline for the evaluation and selection of software engineering tools<br><br>This standard is designed to provide a consistent and coherent framework for the evaluation and selection of software engineering tools. (2015-3-30) |
| ISO/IEC 30130 DIS | Software Engineering | Manufacturers | ISO/IEC 30130 Software engineering – Capabilities of Software Testing Tools<br><br>This International Standard defines the framework to which capabilities of software testing tools are allocated in order to identify the capabilities of products being used by any project for software testing. The framework is defined by objectives of testing, granularity of software to be tested and capabilities. (2015-05-09) |
| ISO/IEC 25022 DIS | Software Engineering | Manufacturers | ISO/IEC DIS 25022 Systems and software Engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of quality in use<br><br>This International Standard is a part of the SQuaRE series of international standards. It provides a set of measures for the characteristics of quality in use (defined in ISO/IEC 25010) that can be used for specifying quality in use requirements (in conjunction with ISO/IEC 25030) and measuring and evaluating quality in use (in conjunction with ISO/IEC 25040 and ISO/IEC 25041). (2015-05-11) |

# STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

| | Topic | Use / Users | Description |
|---|---|---|---|
| ISO/IEC 25024 DIS | Software Engineering | Manufacturers | ISO/IEC DIS 25024 Systems and software Engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of data quality<br><br>This International Standard is a part of the SQuaRE series of international standards. It provides a set of data quality measures that can be used for measuring and evaluating data quality, by referring other SQuaRE series of standards, especially ISO/IEC 25012 SQuaRE – Data quality model. (2015-05-11) |
| ISO/IEC 19770-3 DIS | Information Technology | Manufacturers | ISO/IEC DIS 19770-3 Information technology – IT asset management – Part 3: Software entitlement schema<br><br>This part of ISO/IEC 19770 establishes a set of terms and definitions which may be used by the industry when discussing software entitlements (the key elements within software licenses). It also provides specifications for a file format which enables the digital encapsulation of software entitlements, including associated metrics and their management. (2015-05-09) |
| ISO/IEC 15026-3 DIS | Software Engineering | Manufacturers | *ISO/IEC 15026-3 Systems and software engineering — Systems and software assurance — Part 3: Systems integrity levels*<br><br>This International Standard specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements. (2015-3-20) |

## STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

| | Topic | Use / Users | Description |
|---|---|---|---|
| ISO/IEC 25066 DIS | Software Engineering | Manufacturers | *ISO/IEC 25066 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Common industry Format for Usability — Evaluation Reports*<br><br>This International Standard describes the Common Industry Format (CIF) for reporting usability evaluations. It provides a classification of evaluation approaches and the specifications for the content items in an evaluation reports (content elements). (2015-04-08) |
| ISO/IEC 19770-2 DIS | Software Engineering | Manufacturers | *ISO/IEC 19770-2 Information technology — Software asset management — Part 2: Software identification tag*<br><br>This part of ISO/IEC 19770 provides an International Standard for software identification (SWID) tags. The software identification tag is a standardized data structure containing identification information about a software product that supports new and automated management functions. (2015-04-08) |

## REFERENCES

| | Topic | Use / Users | Description |
|---|---|---|---|
| ONC 10-Year Vision | Health IT | Health IT infrastructure | *ONC 10-Year Vision to Achieve an Interoperable Health IT Infrastructure*<br><br>The document can be found on the SoftwareCPR Standards Navigator web page or at http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf |

| | | | |
|---|---|---|---|
| BSI white paper | Medical devices | Manufacturers | *"The proposed EU regulations for medical and in vitro diagnostic devices"*<br><br>The white paper can be found on the SoftwareCPR Standards Navigator web page |
| EC green paper | Health IT | Manufacturers | *"Green Paper on mobile Health (mHealth)"*<br><br>The green paper can be found on the SoftwareCPR Standards Navigator web page |
| IMDRF SaMD Definitions | Software | Manufacturers | Software as a Medical Device (SaMD): Key Definitions<br>Report on international harmonization of definitions for software as a medical device. Adopted by IMDRF in November.<br><br>***The report can be found on the SoftwareCPR Standards Navigator web page.*** |
| Euro Commission | Medical Devices | Manufacturers | Commission recommendation of 24 September 2013 on the audits and assessments performed by notified bodies in the field of medical devices.<br><br>***The document can be found on the SoftwareCPR Standards Navigator web page.*** |
| FDA Safety communication on cybersecurity | Security | Manufacturers and hospitals | FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations. This safety communication recommends that medical device manufacturers take steps to limit opportunities for unauthorized access to medical devices and hospitals take steps to evaluate network security and protect the hospital systems. The FDA also recommends prompt reporting of events that have impacted the performance of a medical device or hospital network. |
| ICS-CERT Alert regarding medical devices with hard-coded passwords | Security | Manufacturers, hospitals | ICS-CERT is issuing this alert to provide early notice of a report of a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware. The alert also identifies baseline mitigations for reducing risks to these and other cybersecurity attacks. |

| | | | |
|---|---|---|---|
| ONC Patient Safety Action & Surveillance Plan | Health IT safety | Health IT manufacturers, hospitals | The final version of the ONC plan that has the objectives to use health IT to make care safer and to continuously improve the safety of health IT. |
| *ONC contract with the Joint Commission to investigate health IT-related safety events* | Health IT safety | Hospitals, health IT manufacturers | The purpose of this contract is to ensure that there is an early detection system on health IT-related safety issues, including those associated with EHRs. |
| ONC guidance on annual surveillance plans by authorized certification bodies | Surveillance of certified EHRs | Authorized EHR certification bodies | Authorized Certification Bodies are expected to conduct surveillance on EHRs that they have certified. This guidance provides the priorities for topics to assess in the surveillance plan. Safety-related capabilities and security capabilities are two of the four areas for priority identified in this guidance. |
| TEAM-NB position paper on use of ISO 14971:2012 | Risk management | Manufacturers | Describes the steps TEAM-NB members plan to verify where relevant if requirements of EN ISO 14971:2012 have been met. This should help manufacturers update their risk management procedures and files to maintain compliance with the Essential Requirements of the directives, when building on the presumption of conformity.<br><br>***The position paper can be found on the SoftwareCPR Standards Navigator web page.*** |

| | | | |
|---|---|---|---|
| TEAM-NB "Vision on Revision" | Regulation | Regulators, Manufacturers, Notified bodies | This document forms the input of TEAM-NB into the debate on The Revision of European Legislation on Medical Devices. Contributions came from BSI Germany, BSI UK, DEKRA Netherlands, TUV Austria, and TUV Sud.<br><br>***The report can be found on the SoftwareCPR Standards Navigator web page.*** |
| Report | Interoperability | Medical device manufacturers, Hospitals, Regulators | AAMI/FDA Interoperability Summit report<br><br>An AAMI/FDA sponsored summit meeting on medical device interoperability was held in late 2012. This report documents the discussion and identifies themes from the summit.<br><br>This report can be found at http://www.aami.org/interoperability/Interoperability_Summit_publication.pdf |
| Report | Wireless | Hospitals, Medical device manufacturers | AAMI Wireless Workshop report<br><br>A workshop with approximately 80 invited medical wireless experts was held in late 2012. This report documents the discussion and outcomes of this workshop. A follow-up meeting is planned for March 2013.<br><br>This report can be found at http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf |

| | | | |
|---|---|---|---|
| Report | Security | Medical device manufacturers, Regulators | GAO report on FDA review of certain medical devices<br><br>The General Accounting Office does investigations for the US Congress. In this report they reviewed how FDA reviewed implanted medical devices that used wireless communications for security vulnerabilities that could cause safety concerns. They looked at two devices that researchers had shown could be controlled by use of off-the-shelf radio devices. In their findings, they criticized FDA for not reviewing security capabilities in these devices, even though they determined that FDA had the authority to do so. This will certainly result in FDA increasing their scrutiny of security for these type of devices. Since a security vulnerability in a device that is wirelessly communicating over a network seems to surely pose a risk as well, it is likely that FDA will also increase security scrutiny of all devices that use wireless communications.<br><br>Dr. Kevin Fu testified to the National Institute of Standards and Technology Information Security & Privacy Advisory Board that "Conventional malware is rampant in hospitals because of medical devices using unpatched operating systems. There's little recourse for hospitals when a manufacturer refuses to allow OS updates or security patches."<br><br>A report of the meeting can be found in the MIT Technology Review<br>http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/<br><br>The article states that “In September, the Government Accountability Office issued a report warning that computerized medical devices could be vulnerable to hacking, posing a safety threat, and asked the FDA to address the issue. The GAO report focused mostly on the threat to two kinds of wireless implanted devices: implanted defibrillators and insulin pumps. The vulnerability of these devices has received widespread press attention (see "Personal Security" and "Keeping Pacemakers Safe from Hackers"), but no actual attacks on them have been reported.<br><br>Fu, who is a leader in researching the risks described in the GAO report, said those two classes of device are "a drop in the bucket": thousands of other network-connected devices used for patient care are also vulnerable to infection. "These are life-saving devices. Patients are overwhelmingly safer with them than without them. But cracks are showing," he said. (Fu was *Technology Review's* Innovator of the Year in 2009.)”<br><br>One of Dr. Fu’s collaborators in research that showed an implanted defibrillator could be hacked was Dr. William Maisel who is now the Deputy Director for Science at CDRH. FDA staff has indicated that they are in the process of revising the FDA Cybersecurity Guidance. This guidance will likely include recommendations for manufacturer’s security programs for devices and additional recommendations for security information to be provided during pre-market review of devices that are intended for use on a network. In addition, the guidance is now expected to provide information on when a security issue is reportable to the FDA and when a security event will result in a recall.<br><br>Another interesting bit of information in this report was the FDA response that they had hired a consultant (later determined to be McKinsey) to assess how they review software and make suggestions for improvements. This assessment is supposed to be completed by the end of 2012. |

| | | | |
|---|---|---|---|
| Report | Mobile medical devices | Medical devices manufacturers, Hospitals, Regulators | FCC report on Mobile Medical Devices<br><br>The FCC created an independent mHealth Task Force, to research the barriers to rapid deployment of mHealth technology and develop recommendations to government and industry to address those barriers. This report documents the task force recommendations for achieving 5 goals:<br>Goal 1: FCC should continue to play a leadership role in advancing mobile health adoption.<br>Goal 2: Federal agencies should increase collaboration to promote innovation, protect patient safety, and avoid regulatory duplication.<br>Goal 3: The FCC should build on existing programs and link programs where possible in order to expand broadband access for healthcare.<br>Goal 4: The FCC should continue efforts to increase capacity, reliability, interoperability and RF safety of mHealth technologies.<br>Goal 5: Industry should support continued investment, innovation, and job creation in the growing mobile health sector.<br><br>Recommendations include:<br>• greater collaboration with other US Federal agencies<br>• promoting the availability of broadband for healthcare<br>• harmonizing spectrum allocations for healthcare internationally<br>• industry use of standards based technologies for transmitting authenticated messages and encrypted health information<br><br>***This report can be found on the Standards Navigator web page*** |
| Report | Health IT | Hospitals, EHR vendors, MD manufacturers | Institute of Medicine report – Health IT and patient safety<br><br>The Institute of Medicine produced a report on the impact of Health IT on patient safety. The report had a number of recommendations for the Secretary of HHS.<br><br>***A presentation on the recommendations and the entire report are available at the SoftwareCPR Standards Navigator web page.*** |

| | | | |
|---|---|---|---|
| Regulation | Regulation | Medical device manufacturers, IVD manufacturers | EU draft proposed new Medical Device Regulation and In-Vitro Device Regulation<br><br>These draft regulations can be found at<br>http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf - medical devices<br><br>http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_541_en.pdf - In-vitro devices |

## STANDARDS CURRENTLY UNDER DEVELOPMENT OR REVISION

| | Topic | Use / Users | Description |
|---|---|---|---|
| IEC 62304 Amendment 1 | Software Life Cycle | Medical Device manufacturers, Regulators | Amendment to the Medical Device Software Life Cycle standard. This standard is harmonized in the EU. The amendment addresses software safety classification and how to be compliant with legacy software.<br><br>Current status: Comments received on the CDV have been resolved and the FDIS is being edited by IEC.<br><br>Expected completion: mid 2015 |
| IEC 82304-1 | Health Software | Medical device manufacturers, Regulators | New standard on Health Software: General Requirements. This standard is intended to be for standalone software products and to cover the product level requirements such as product validation, labeling, documents to be provided to the user, etc.<br><br>Current status: Comments received on the second CD are being resolved.<br><br>Next step: A CDV is expected to be circulated in early 2015.<br><br>Expected completion: end of 2015 |
| ISO 13485 | Medical devices | Medical device manufacturers, Regulators | The Quality Management System standard is being revised to bring it into alignment with ISO 9001:2008.<br><br>Next step: Second DIS is currently out for ballot.<br><br>Expected completion: 2016 |